

FILED

2013 MAR -7 AM 11:55

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

U.S. DISTRICT COURT
MIDDLE DISTRICT OF TN

GENESCO INC.,

Plaintiff,

vs.

VISA U.S.A. INC.; VISA INC.; and
VISA INTERNATIONAL SERVICE
ASSOCIATION,

Defendants.

Civil Action No. _____

COMPLAINT

Plaintiff Genesco Inc. ("Genesco"), by its undersigned attorneys, as and for its Complaint, alleges the following:

NATURE OF THE ACTION

1. Genesco brings this Complaint against Defendants Visa U.S.A. Inc., Visa Inc., and Visa International Service Association (collectively "Visa") to recover \$13,298,900.16 in non-compliance fines and issuer reimbursement assessments that Visa wrongfully imposed on and collected from Wells Fargo Bank, N.A ("Wells Fargo Bank") and Fifth Third Financial Corporation ("Fifth Third Bank," and together with Wells Fargo Bank, the "Acquiring Banks"), and that the Acquiring Banks in turn collected from Genesco pursuant to Genesco's contractual obligation to indemnify the Acquiring Banks against such wrongful assessments. The Complaint also seeks to recover incidental damages incurred directly by Genesco, or incurred by the Acquiring Banks and indemnified by Genesco, as a result of Defendants' wrongful conduct in imposing and collecting the non-compliance fines and issuer reimbursement assessments. Visa

breached its contracts with the Acquiring Banks and violated applicable law by imposing and collecting the non-compliance fines and issuer reimbursement assessments, because the non-compliance fines and issuer reimbursement assessments are not authorized by the Visa International Operating Regulations in effect at the time of the inception of the data security breach that is the subject of the Complaint (the "VIOR"), which are incorporated into the agreements between Visa and the Banks, and in any event constitute unenforceable penalties for breach of contract. As its basis for recovering the amounts sought by the Complaint, Genesco asserts breach of contract claims against Visa in Genesco's capacity as assignee of and subrogee to Wells Fargo Bank's rights and as subrogee to the rights of Fifth Third Bank. In the alternative, Genesco asserts statutory and equitable claims in its own right against Visa as grounds for recovering the amounts in question.

PARTIES

2. Plaintiff is Genesco Inc. ("Genesco"), a Tennessee corporation with its principal place of business located in Nashville, Tennessee. Genesco is a specialty retailer which sells footwear, headwear, sports apparel and accessories in more than 2,440 retail stores throughout the U.S., Canada, the United Kingdom and the Republic of Ireland, principally under the names Journeys, Journeys Kidz, Shi by Journeys, Underground by Journeys, Schuh, Lids, Lids Locker Room, Johnston & Murphy, and on internet websites.

3. Defendant Visa, Inc., a Delaware stock corporation with its principal place of business in San Francisco, California, operates a payment system pursuant to which Visa contracts with financial institutions for the purpose of enabling those institutions to offer their customers (cardholders and merchants) the ability to conduct payment transactions by means of credit and debit cards (jointly, "payment cards") bearing the Visa logo.

4. Defendant Visa U.S.A. Inc. ("Visa USA"), a Delaware membership corporation with its principal place of business in San Francisco, California, is the principal operating subsidiary in the United States of Visa, Inc., a Delaware stock corporation. Visa USA operates a retail electronic payments network in the United States which supports payment programs offered by member financial institutions to businesses and consumers.

5. Defendant Visa International Service Association ("Visa International"), a Delaware membership corporation with its principal place of business in San Francisco, California, is a wholly owned subsidiary of Visa, Inc. which owns and operates a global processing platform that provides processing services for payment cards.

6. Visa derives substantial revenues from transactions occurring in this judicial district, such as credit card purchases and debit card purchases made with Visa branded payment cards.

JURISDICTION AND VENUE

7. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332. The matter in controversy exceeds, exclusive of interest and costs, \$75,000 and is not between citizens of the same state.

8. Venue in this district is proper pursuant to 28 U.S.C. § 1391.

GENERAL ALLEGATIONS

Genesco's Relationship with Visa, Wells Fargo Bank, and Fifth Third Bank

9. A financial institution that wants to offer its customers the ability to make or accept payments via Visa-branded payment cards is required to enter into a license agreement with Visa authorizing the institution to participate in the Visa network as a "Visa Member." Visa Members participate in the Visa network by acting as "issuers" or as "acquirers" (or both). Visa issuers authorize cardholders (by contract) to use Visa-branded payment cards to make

payment transactions, and Visa acquirers in turn authorize merchants (again, by contract) to accept Visa-branded payment cards in payment for transactions. Each day there is a funds flow within the Visa network whereby the dollar amount of a participating merchant's Visa-branded payment card transactions is paid to the merchant by its Visa acquirer, and the acquirer collects that amount back from Visa, which in turn collects the amount back from the relevant Visa issuers, which ultimately collect the amount back from the Visa cardholders who made the transactions in question with the participating merchant.

10. Genesco accepts Visa-branded payment cards in payment for transactions made at its stores. Wells Fargo Bank, a Visa Member, is Genesco's acquirer for Visa Credit Card and Non-PIN Debit Card transactions, which are processed by Wells Fargo Merchant Services, LLC (together with Wells Fargo Bank, "Wells Fargo"). Fifth Third Bank, a Visa Member, is Genesco's acquirer for Visa PIN Debit Card transactions, which are processed by Vantiv, formerly Midwest Payment Systems (and together with Fifth Third Bank, "Fifth Third"). Genesco's contract with Wells Fargo (the "Wells Fargo Agreement") is governed by the laws of the State of New York. Genesco's contract with Fifth Third (the "Fifth Third Agreement" and, together with the Wells Fargo Agreement, the "Acquiring Bank Agreements") is governed by the laws of the State of Ohio.

11. Under the Acquiring Bank Agreements, in exchange for the Acquiring Banks' enabling and facilitating Genesco's participation in the Visa network, Genesco agreed to comply with the VIOR, insofar as they apply to merchants, and to pay the Acquiring Banks an "interchange fee" equal to a percentage of the dollar value of each Visa transaction completed at a Genesco store. The Acquiring Banks keep a portion of Genesco's interchange fees for themselves and pay the rest of those fees to Visa under their contract with Visa. Visa in turn

keeps for itself a portion of what it is paid by the Acquiring Banks and, pursuant to its separate contracts with its issuers, pays the rest of Genesco's interchange fees to the Visa issuers that issued the Visa accounts that were used to make the transactions in question at Genesco's stores.

12. Under the Acquiring Bank Agreements, Genesco agreed to indemnify the Acquiring Banks against certain assessments that Visa might purport to impose on the Acquiring Banks under the VIOR related to Visa transactions completed at Genesco stores, even in cases where Visa violated the VIOR or otherwise violated the law by imposing the assessment(s) in question.

13. The relevant indemnification provision in the Fifth Third Agreement states: "Notwithstanding any other provision of this Agreement, Merchant shall be responsible for all fees, assessments and penalties imposed by third party providers such as, but not limited to, VISA, MasterCard, Other Networks and telecommunication companies, and any changes or increases shall automatically become effective without notice and shall be immediately payable by [Genesco] when assessed by [Fifth Third]." Fifth Third Agreement, Section 13.

14. The indemnification provision in the Wells Fargo Agreement states: "You agree to pay any fines imposed on us by any Association resulting from Chargebacks and any other fees or fines imposed by an Association with respect to your acts or omissions" and "You agree to indemnify and hold us harmless from and against all losses, liabilities, damages and expenses ... arising out of any third party indemnifications we are obligated to make as a result of your actions (including indemnification of any Association or Issuer)." Wells Fargo Agreement, Sections 18.9, 26.1.d.

The Payment Card Industry Data Security Standards

15. The VIOR require all acquirers to cause their merchants to comply with the Payment Card Industry Data Security Standards ("PCI DSS"). *See* VIOR ID#: 081010-010410-0003356. The PCI DSS is a set of payment card account data security requirements developed by the card brands (including Visa) that founded the Payment Card Industry Security Standards Council. The PCI DSS include twelve overarching security Requirements, each of which is split into numerous security sub-requirements, for a total of over 200 security sub-requirements. The alleged intent of the PCI DSS, according to the card brands, is to protect payment card account data (such as the account number, the expiration date, and the card verification codes embedded in the card's magnetic stripe (the "CVC") and printed on the back of the card (the "CVC2")) from being stolen from merchants that handle such data and then being used by the thieves (often by means of creating a counterfeit of the accountholder's card) to make fraudulent transactions on the account in question.

16. The PCI DSS apply to all system components of any entity that is subject to the PCI DSS. In the context of PCI DSS, "system components" are defined as any network component, server, or application that is included in or connected to the "cardholder data environment." The cardholder data environment is comprised of people, processes and technology that store, process or transmit cardholder data or sensitive authentication data on behalf of an entity. An entity that is subject to the PCI DSS may reduce the scope of its PCI DSS compliance obligation by employing network segmentation to limit the "system components" within the entity's network that are included in or connected to the entity's "cardholder data environment" and that, accordingly, are subject to the PCI DSS.

Criminal Intrusion into Genesco's Computer Network

17. In 2010, Genesco was the victim of a sophisticated cybercrime attack (the "Intrusion") in which the intruder(s) sought to steal payment card data from Genesco's computer network.

18. The criminals who perpetrated the Intrusion attempted to take advantage of a particular feature of the PCI DSS security protocols which govern how payment card transactions are currently conducted in the United States. Today, most payment card transactions are initiated by means of the accountholder's payment card being "swiped" at the point of sale (a "mag-stripe-swipe transaction"). During the transaction authorization process for a mag-stripe-swipe transaction, certain payment card account data embedded in the card's magnetic stripe (including the account number, the card's expiration date, and – most importantly – the card's CVC) is electronically transmitted from the merchant to its acquirer, and then from the acquirer to the card brand (e.g., Visa), and then from the card brand to the issuer, so that the issuer can determine whether or not to approve the transaction.

19. The feature of the payment card system that the criminals sought to exploit in the Intrusion is that, according to PCI DSS security protocols and consistent with longstanding and pervasive industry practice, the payment card account data required for approval of a mag-stripe-swipe transaction is permitted to be transmitted *in unencrypted form* during the transaction approval process. *Unencrypted* payment card data of this sort is highly sought after by criminals, because the unencrypted version of the payment card account data required for approval of a mag-stripe-swipe transaction can potentially be used to create a counterfeit of the payment card in question, which counterfeit card can then potentially be used to make fraudulent transactions on the account in question. Notwithstanding this circumstance, the PCI DSS not only does not

prohibit, it actually expressly approves, unencrypted transmission of mag-stripe-swipe transaction approval data. The VIOR, consistent with this aspect of the PCI DSS, do not prohibit retention of unencrypted mag-stripe-swipe transaction approval data during the authorization process for a transaction. *See* VIOR ID#: 081010-010410-0002228.

20. In the Intrusion, the criminals sought to steal payment card account data as it was being transmitted by Genesco to Fifth Third and Wells Fargo, in accordance with industry standards and the PCI DSS, in unencrypted form during the approval process. The criminals did this by inserting into Genesco's computer network malicious software ("malware") that employed "packet sniffer" technology custom designed to acquire account data while the data was in transit through Genesco's computer network on its way to Fifth Third or Wells Fargo for transaction approval.

21. During the course of the Intrusion, the thieves did not target, nor did the thieves access, any *stored* payment card account information located on Genesco's computer network.

22. Following the Intrusion, Visa issued a Compromise Account Management Systems Alert ("CAMS Alert") to its issuers with respect to every Visa account that was processed through the Genesco cardholder data environment during the period from December 4, 2009 through December 1, 2010 (collectively, "Alerted-On Accounts"), even though there was no forensic evidence that any of the Alerted-On Accounts had been compromised in the Intrusion, and even though the forensic evidence affirmatively showed that some of the Alerted-On Accounts *were not* compromised during the Intrusion.

**Visa's Account Data Compromise Recovery Process
and Data Compromise Recovery Solution**

23. The VIOR contain two processes by which an acquirer can incur contractual liability to Visa for losses incurred by Visa issuers in the event one of the acquirer's merchants

suffers a data security breach involving its cardholder data environment: the Account Data Compromise Recovery (“ADCR”) and the Data Compromise Recovery Solution (“DCRS”) processes.

24. In the event one of a Visa acquirer’s merchants suffers a data security breach involving its cardholder data environment, ADCR purports to be a contractual mechanism for (a) determining whether the data security breach in question resulted in an “account compromise event” with respect to any particular Visa accounts issued by U.S. issuers and, if so, whether the merchant in question (and hence its acquirer) bears responsibility for that event; (b) determining the counterfeit fraud losses and operating expenses that U.S. Visa issuers incurred as a result of the account compromise event, and (c) Visa’s collecting the contractually specified portion of those losses from the Visa acquirer in question. A Visa acquirer’s potential liability to Visa under the ADCR process (“ADCR Recovery”) includes two components: Counterfeit Fraud Recovery and Operating Expense Recovery.

25. Under Counterfeit Fraud Recovery, a Visa acquirer is potentially contractually liable to Visa for a portion of any counterfeit fraud losses incurred by U.S. Visa issuers as a result of a magnetic-stripe-data account compromise event suffered by one of the acquirer’s merchants. Under the VIOR, an acquirer has potential contractual liability for Counterfeit Fraud Recovery only when (1) an “account compromise event” involving the full contents of any track on the card’s magnetic stripe occurs with respect to at least 10,000 particular U.S.-issued Visa accounts; (2) a CAMS Alert covering the particular Visa accounts that suffered the account compromise event is sent to the issuers of those Visa accounts; (3) “incremental fraud” is attributable to the particular Visa accounts that suffered the account compromise event; and (4) the merchant in question has committed at least one of the following PCI DSS violations: (a)

stored the full contents of any track on the magnetic stripe subsequent to authorization of a transaction and thereby allowed the compromise of the full contents of any track on the magnetic stripe of the particular Visa accounts that suffered the account compromise event, (b) committed some other violation of the PCI DSS that could have allowed the compromise of the full contents of any track on the magnetic stripe of the particular Visa accounts that suffered the account compromise event, or (c) committed a violation of the PIN Management Requirements Documents that could have allowed a compromise of PIN data of the particular Visa accounts that suffered the account compromise event subsequent to authorization of transactions on those accounts.

26. The VIOR do not define “account compromise event” for purposes of ADCR. However, Visa interprets the term account compromise event, as applied to any particular Visa account for ADCR purposes, as an *actual theft* of cardholder data relative to that account (as opposed to the mere possibility of such theft). Moreover, even apart from Visa’s interpretation of the term, the only reasonable (or at a minimum the most reasonable) interpretation of the term “account compromise event” as applied to any particular Visa account for ADCR purposes is as meaning an actual theft of cardholder data relative to that account (as opposed to the mere possibility of such theft).

27. The VIOR define “incremental fraud”, for purposes of ADCR, as the portion (if any) of the counterfeit fraud reported on the particular U.S.-issued Visa accounts that suffered an account compromise event that is above the “baseline counterfeit fraud level” for those accounts during the period in question. The term “baseline counterfeit fraud level” is not defined in the VIOR, but for ADCR purposes Visa interprets that term to refer to the amount of counterfeit fraud that normally would have been expected to have been reported on the accounts in question

for the period in question, taking into account the rampant counterfeit fraud that any particular account, or group of accounts, in the Visa system is subject to at any given point in time. Moreover, even apart from Visa's interpretation of the term, the only reasonable (or at a minimum the most reasonable) interpretation of the term "baseline counterfeit fraud level" as applied for ADCR purposes to any particular group of Visa accounts is as meaning the amount of counterfeit fraud that normally would have been expected to have been reported on the accounts in question for the period in question.

28. Under the VIOR, then, a Visa acquirer cannot have contractual liability to Visa for Counterfeit Fraud Recovery with respect to the activities of one of its merchants unless (1) the merchant suffered a theft of cardholder data with respect to not less than 10,000 particular U.S.-issued Visa accounts, (2) the merchant committed a PCI DSS violation that allowed (or at a minimum could have allowed) the theft to occur, and (3) the compromised group of Visa accounts thereafter incurred an amount of counterfeit fraud in excess of the amount of counterfeit fraud that normally would have been expected to have been reported on the accounts in question for the period in question.

29. Under Operating Expense Recovery, a Visa acquirer is potentially contractually liable to Visa for a portion of any operating expenses incurred by U.S. Visa issuers as a result of a magnetic-stripe-data account compromise event suffered by one of the acquirer's merchants. Under the VIOR, an acquirer has potential contractual liability for Operating Expense Recovery only when (1) an account compromise event involving the full contents of any track on the card's magnetic stripe occurs with respect to at least 10,000 particular U.S.-issued Visa accounts; (2) a CAMS Alert covering the particular Visa accounts that suffered the account compromise event is sent to the issuers of those accounts; and (3) the merchant in question has committed at least one

of the following PCI DSS violations: (a) stored the full contents of any track on the magnetic stripe subsequent to authorization of a transaction and thereby allowed the compromise of the full contents of any track on the magnetic stripe of the particular Visa accounts that suffered the account compromise event, (b) committed some other violation of the PCI DSS that could have allowed the compromise of the full contents of any track on the magnetic stripe of the particular Visa accounts that suffered the account compromise event, or (c) committed a violation of the PIN Management Requirements Documents that could have allowed a compromise of PIN data for a Visa Transaction, a Plus transaction, or an Interlink transaction subsequent to authorization.

30. Under the VIOR, then, a Visa acquirer cannot have contractual liability to Visa for Operating Expense Recovery with respect to the activities of one of its merchants unless (1) the merchant suffered a theft of cardholder data with respect to not less than 10,000 particular U.S.-issued Visa accounts, and (2) the merchant committed a PCI DSS violation that allowed (or at a minimum could have allowed) the theft to occur. Moreover, even in that event the VIOR provide that a Visa acquirer can have contractual liability to Visa for Operating Expense Recovery with respect to the activities of one of its merchants only if, and only to the extent, operating expenses are in fact incurred by the issuers of the Visa accounts in question as a result of the theft in question.

31. In the event one of a Visa acquirer's merchants suffers a data security breach involving its cardholder data environment, DCRS purports to be a contractual mechanism for (a) determining whether the data security breach in question has resulted in a theft of cardholder data relative to any particular Visa accounts issued by non-U.S. issuers and, if so, whether the merchant in question (and hence its acquirer) bears responsibility for that theft; (b) determining the counterfeit fraud losses that non-U.S. Visa issuers incurred as a result of that theft, and (c)

Visa's collecting the contractually specified portion of those losses from the Visa acquirer in question.

32. Under the VIOR, an acquirer has potential contractual liability to Visa under the DCRS process only when (1) a "data compromise event" involving the theft of full-magnetic stripe data occurs with respect to at least 10,000 particular Visa accounts issued by non-U.S. Visa issuers; (2) the data compromise event involves a combined total of \$100,000 or more of full-magnetic stripe counterfeit fraud having occurred during the period in question on the particular Visa accounts that were compromised in the event; (3) "incremental fraud" is attributable to the particular Visa accounts that suffered the data compromise event; and (4) the merchant in question has committed a violation of the PCI DSS that could have allowed the theft of the full contents of any track on the magnetic stripe of the particular Visa accounts that suffered the data compromise event.

33. The VIOR do not define the term "data compromise event" for purposes of DCRS. However, Visa interprets the term data compromise event, as applied to any particular Visa account for DCRS purposes, as an actual theft of cardholder data relative to that account (as opposed to the mere possibility of such theft). Moreover, even apart from Visa's interpretation of the term, the only reasonable (or at a minimum the most reasonable) interpretation of the term "data compromise event" as applied to any particular Visa account for DCRS purposes is as meaning an actual theft of cardholder data relative to that account (as opposed to the mere possibility of such theft).

34. The VIOR do not define the term "incremental fraud", for purposes of DCRS. However, for purposes of DCRS Visa interprets that term as the portion (if any) of the counterfeit fraud reported on the particular non-U.S.-issued Visa accounts that suffered the data

compromise event in question that is above the amount of counterfeit fraud that normally would have been expected to have been reported on the accounts in question for the period in question, taking into account the rampant counterfeit fraud that any particular account, or group of accounts, in the Visa system is subject to at any given point in time. Moreover, even apart from Visa's interpretation of the term, the only reasonable (or at a minimum the most reasonable) interpretation of the term "incremental fraud" as used in the DCRS, as applied to any particular group of non-U.S.-issued Visa accounts, is as meaning the counterfeit fraud reported on those accounts that is above the amount of counterfeit fraud that normally would have been expected to have been reported on those accounts for the period in question.

35. Under the VIOR, then, a Visa acquirer cannot have contractual liability to Visa under the DCRS process with respect to the activities of one of its merchants unless (1) the merchant suffered a theft of cardholder data with respect to not less than 10,000 particular non-U.S.-issued Visa accounts, (2) the merchant committed a PCI DSS violation that allowed (or at a minimum could have allowed) the theft to occur, and (3) the compromised group of Visa accounts thereafter incurred an amount of counterfeit fraud in excess of the amount of counterfeit fraud that normally would have been expected to have been reported on the accounts in question for the period in question.

Reserve Agreement between Wells Fargo and Genesco

36. On April 21, 2011, Genesco, Wells Fargo, and Wells Fargo Merchant Services, L.L.C. entered into a Reserve Agreement under which Genesco agreed to fund a reserve account with regard to potential fines, issuer fraud and operating expense assessments and/or other assessments anticipated to be imposed on Wells Fargo by Visa pursuant to the VIOR in regard to the Intrusion.

37. In the Reserve Agreement, Genesco acknowledged that it had an obligation to indemnify Wells Fargo for the amount of any such assessments, regardless of whether or not the assessment in question was valid under the VIOR or under relevant applicable law.

38. In the Reserve Agreement, Wells Fargo agreed that, upon having been reimbursed by Genesco for the amount of any such fine or assessment out of the reserve account or otherwise, Wells Fargo would be deemed to have assigned, transferred, and conveyed to Genesco any and all rights, claims or causes of actions that Wells Fargo may have against Visa to obtain reimbursement of any portion of such fine or assessment and that Genesco would be deemed to be fully subrogated to any and all such rights, claims or causes of actions.

The Assessments

39. By letters dated May 31, 2011, Visa notified Wells Fargo and Fifth Third that it had determined that each Acquiring Bank was non-compliant with the PCI DSS and the VIOR's Cardholder Information Security Program ("CISP") as a result of the Intrusion and that each Acquiring Bank had been assessed a fine of \$5,000 (the "Non-Compliance Fines").

40. By letters dated November 8, 2011, Visa notified Wells Fargo and Fifth Third that it had determined that the Intrusion qualified for the ADCR process and had determined the total ADCR liability of Wells Fargo and Fifth Third in regard to the Intrusion to be \$5,167,714.58 (the "ADCR Assessment"), comprised of \$2,773,536.00 in Operating Expense Recovery (the "Operating Expense Recovery Assessment") and \$2,394,178.58 in Counterfeit Fraud Recovery (the "Counterfeit Fraud Recovery Assessment").

41. By letter dated November 8, 2011, Visa notified Wells Fargo that it had determined that the Intrusion qualified for the DCRS process and had determined the total DCRS liability of Wells Fargo in regard to the Intrusion to be \$8,121,185.58 (the "DCRS Assessment").

42. On or about June 17, 2011, Visa collected \$5,000 from each of the Acquiring Banks in Non-Compliance Fines. Wells Fargo transferred \$5,000 from the Genesco reserve account in reimbursement for the Non-Compliance Fine pursuant to the terms of the Wells Fargo Agreement and the Reserve Agreement. Fifth Third withheld \$5,000 from settlement funds otherwise due to Genesco in reimbursement for the Non-Compliance Fine pursuant to the terms of the Fifth Third Agreement.

43. On or about January 5, 2013, Visa collected \$2,301,693.53 in Counterfeit Fraud Recovery, \$1,573,785.60 in Operating Expense Recovery, and the \$8,121,185.58 DCRS Assessment from Wells Fargo (the "Wells Fargo Assessments"). Wells Fargo transferred \$11,996,664.71 from the Genesco reserve account in reimbursement for the Wells Fargo Assessments pursuant to the terms of the Wells Fargo Agreement and the Reserve Agreement.

44. On or about January 5, 2013, Visa collected \$142,659.53 in Counterfeit Fraud Recovery and \$1,199,750.40 in Operating Expense Recovery from Fifth Third (the "Fifth Third Assessments," and together with the Wells Fargo Assessments, the "Assessments"). Fifth Third withheld \$1,342,409.93 from settlement funds otherwise due to Genesco in reimbursement for the Fifth Third Assessments pursuant to the terms of the Fifth Third Agreement.

45. In calculating the amounts of the Operating Expense Recovery Assessment, the Counterfeit Fraud Recovery Assessment, and the DCRS Assessment, Visa found certain of the Alerted-On Accounts to be *ineligible* for the ADCR and DCRS processes, even though they had been included in the CAMS Alerts that Visa issued relative to the Intrusion, because the forensic evidence showed that those accounts *had not* been compromised during the Intrusion. However, Visa found certain other of the Alerted-On Accounts to be *eligible* for the ADCR and DCRS processes even though the forensic evidence showed that those accounts likewise *had not* been

compromised during the Intrusion. Moreover, Visa found still other of the Alerted-On Accounts to be *eligible* for the ADCR and DCRS processes even though there was no forensic evidence showing that those accounts had been compromised during the Intrusion.

Visa's Invalid Imposition of the Non-Compliance Fines

46. The May 31, 2011 notices to Wells Fargo and Fifth Third state that the Non-Compliance Fines were imposed pursuant to ID# 041010-41010-0008031 of the VIOR, and that the amount of the Non-Compliance Fines had been calculated in accordance with ID# 021010-041010-0009032 of the VIOR. These notices also informed Fifth Third and Wells Fargo that under ID#: 010410-010410-0007289 of the VIOR that they had 30 days from the receipt of the notices to submit an appeal to Visa.

47. By letter dated June 30, 2011, Fifth Third appealed the Non-Compliance Fine issued by Visa against Fifth Third. By letter dated July 6, 2011, Wells Fargo appealed the Non-Compliance Fine issued by Visa against Wells Fargo. Visa has not ruled on either appeal, and it continues to hold (now nearly two years later) the \$10,000 in Non-Compliance Fines that it collected in 2011.

48. Visa's imposition of the Non-Compliance Fines is a violation of Visa's contract with Fifth Third and a violation of Visa's contract with Wells Fargo because at the time of the Intrusion and at all other relevant times Genesco was in compliance with the PCI DSS requirements and, as a result, neither Fifth Third nor Wells Fargo was at any relevant time in violation of its contractual obligation to Visa to cause Genesco to maintain compliance with the PCI DSS requirements. Indeed, at the time Visa imposed the Non-Compliance Fines, Visa had no reasonable basis for concluding that Genesco was non-compliant with the PCI DSS requirements at the time of the Intrusion or at any other relevant time.

49. Further, Visa breached its contracts with Fifth Third and Wells Fargo by imposing the Non-Compliance Fines because Visa did not comply with the notice and enforcement procedures of the VIOR in doing so. The VOIR's "Fines and Penalties Process" section details four distinct steps Visa must follow in any fine assessment: (1) Allegation of a violation brought by a Member or Visa officer (ID# 010410-010410-0007366); (2) Investigation of the allegations by Visa, including the issuance of a Notification to the Member under investigation (ID# 010410-010410-0007366); (3) Determination of a violation, based on the Member's response to the Notification or the Member's failure to respond (ID# 010410-010410-0001052); and (4) Notification of Visa's determination that a violation occurred, that a fine is being assessed, and that the Member has a right of appeal (ID# 010410-010410-0001054). Each step is dependent on the preceding steps.

50. The Non-Compliance Fines were not predicated on allegations that were brought by a member or a Visa officer, as required by ID# 010410-010410-0007366. Moreover, prior to imposing the Non-Compliance Fines, the Visa staff never sent a notification to either Fifth Third or Wells Fargo, as required by ID# 010410-010410-0007366. Nor did the Visa staff offer or permit Fifth Third or Wells Fargo an opportunity to respond to the allegations under investigation prior to purporting to determine that they had violated the VIOR and therefore would be subject to the Non-Compliance Fines, as required by ID# 010410-010410-0001052. Since a determination that a violation has occurred can only be based on a member's response to the notification, Visa could not possibly have had a valid basis under the VIOR for imposing the Non-Compliance Fines, even if Fifth Third and/or Wells Fargo had at some relevant time violated its contractual obligation to Visa to cause Genesco to maintain compliance with the PCI DSS requirements (which neither of them did).

51. In any event, the Non-Compliance Fines would be legally unenforceable even if they were valid under the VIOR, because the Non-Compliance Fines constitute a penalty – rather than damages – for the Acquiring Banks’ allegedly having breached their contracts with Visa, and as such they are legally unenforceable under applicable law. Visa does not even pretend that the Non-Compliance Fines represent the actual damages Visa incurred by reason of the Acquiring Banks’ alleged failure to cause Genesco to maintain compliance with the PCI DSS requirements. Moreover, the Non-Compliance Fines cannot be sustained as constituting liquidated damages by reason of the Acquiring Banks’ alleged breach of this contractual obligation, because (1) the VIOR afford Visa unbounded discretion regarding the imposition and amounts of the Non-Compliance Fines; (2) the amount of the Non-Compliance Fines does not bear a reasonable relationship to any harm that Visa might suffer as a result of a violation of the Acquiring Banks’ obligation to cause Genesco to maintain compliance with the PCI DSS requirements; and (3) the Non-Compliance Fines are not Visa’s exclusive damages remedy by reason of the Acquiring Banks’ alleged violation of that obligation. Because the Non-Compliance Fines cannot be sustained as a valid award of either actual or liquidated damages by reason of Acquiring Banks’ alleged breaches of their contractual obligation to Visa to cause Genesco to maintain compliance with the PCI DSS requirements, the Non-Compliance Fines necessarily constitute a penalty by reason of such alleged breaches, and as such they are unenforceable under applicable law regardless of whether they comport with the VIOR.

Visa’s Invalid Imposition and Collection of the Counterfeit Fraud Recovery Assessment

52. The Counterfeit Fraud Recovery Assessment directly violated the VIOR because Visa did not show (and indeed could not even reasonably have concluded), and in any event it was not the case, that (1) Genesco suffered a theft of cardholder data with respect to all the U.S.-

issued Alerted-On Accounts that Visa found to be eligible for the ADCR process (or for that matter even with respect to any particular U.S.-issued Alerted-On Account that Visa found to be so eligible); (2) Genesco committed a PCI DSS violation that allowed the theft of cardholder data with respect to all the U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process (or for that matter even with respect to any particular U.S.-issued Alerted-On Account that Visa found to be so eligible); and/or (3) the U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process (or for that matter any particular portion of the U.S.-issued Alerted-On Accounts that Visa found to be so eligible) thereafter incurred, as a group, an amount of counterfeit fraud in excess of the amount of counterfeit fraud that normally would have been expected to have been reported on that group of accounts for the period in question.

53. In regard to Paragraph 52(1) above, under the VIOR an account can be made eligible for Counterfeit Fraud Recovery pursuant to the ADCR process only if it suffers an "account compromise event." The term "account compromise event", as used in the ADCR, means an actual theft of cardholder data relative to the account in question. Visa did not show (and indeed could not even reasonably have concluded), and in any event it was not the case, that Genesco suffered a theft of cardholder data with respect to all the U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process (or for that matter even with respect to any particular U.S.-issued Alerted-On Account that Visa found to be so eligible). Indeed, with respect to some of the U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process, Visa found the Alerted-On Account in question to be so eligible even though the forensic evidence affirmatively showed that those accounts *had not* been compromised during the Intrusion. Moreover, with respect to all of the other U.S.-issued

Alerted-On Accounts that Visa found to be eligible for the ADCR process, Visa found the Alerted-On Account in question to be so eligible even though there was no forensic evidence showing that those accounts had been compromised during the Intrusion. Accordingly, with respect to all (or at a minimum some) of the U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process, Visa did not show (and indeed could not even reasonably have concluded), and in any event it was not the case, that Genesco suffered an account compromise event as to those accounts. The Counterfeit Fraud Recovery Assessment thus violated the VIOR because all (or at a minimum some) of the Visa accounts on which the assessment is based were ineligible for the ADCR process by reason of their not having suffered an account compromise event.

54. Moreover, in further regard to Paragraph 52(1) above, certain of the U.S.-issued Alerted-On Accounts on which the Counterfeit Fraud Recovery Assessment is based could not even *possibly* have suffered an account compromise event during the course of the Intrusion, because reboots of the intruded-upon servers in the Genesco cardholder data environment caused any log files that may have contained data relative to those accounts to be overwritten by the intruder(s)' malware prior to the intruder(s)' having an opportunity to exfiltrate those files from Genesco's network. Thus, even if the term "account compromise event" as used in the ADCR means merely a *possible* theft of cardholder data relative to the account in question, and not an *actual* theft of such data (which is not the case), as a result of such overwriting Genesco did not even suffer a *possible* theft of cardholder data with respect to many of the U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process. For this reason as well, then, the Counterfeit Fraud Recovery Assessment violated the VIOR because even under a broad definition of the term "account compromise event" at least some of the U.S.-issued Alerted-On

Accounts on which the assessment is based were ineligible for the ADCR process by reason of their not having suffered such an event.

55. In regard to Paragraph 52(2) above, under the VIOR a Visa account can be made eligible for Counterfeit Fraud Recovery pursuant to the ADCR process only if the entity in question committed some violation of the PCI DSS that could have allowed the compromise (i.e., the theft) of the full contents of any track on the magnetic stripe of that particular account. Here, Visa did not show (and indeed could not even reasonably have concluded), and in any event it was not the case, that Genesco committed a PCI DSS violation that allowed the theft of cardholder data with respect to all the U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process (or for that matter even with respect to any particular U.S.-issued Alerted-On Account that Visa found to be so eligible). In particular, Visa did not show (and indeed could not even reasonably have concluded), and in any event it was not the case, that any PCI DSS violation on the part of Genesco is what enabled the intruder(s) to enter Genesco's computer network or is what enabled them potentially to steal payment card account data from Genesco's computer system. The Counterfeit Fraud Recovery Assessment thus violated the VIOR because all of the U.S.-issued Alerted-On Accounts on which the assessment is based were ineligible for the ADCR process by reason of their having been no PCI DSS violation by Genesco that could have allowed the compromise (i.e., the theft) of the full contents of any track on the magnetic stripe of that particular account.

56. In regard to Paragraph 52(3) above, under the VIOR a group of Visa accounts can form the basis for a Visa acquirer to be liable for Counterfeit Fraud Recovery pursuant to the ADCR process only where "incremental fraud" is attributable to that particular group of accounts. Moreover, under the VIOR "incremental fraud" can properly be attributed to a

particular group of Visa accounts only where that group of accounts incurred an amount of counterfeit fraud in excess of the amount of counterfeit fraud that normally would have been expected to have been reported on the accounts in question for the period in question. Visa did not show (and indeed could not even reasonably have concluded), and in any event it was not the case, that the U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process (or for that matter any particular portion of the U.S.-issued Alerted-On Accounts that Visa found to be so eligible) incurred, as a group, an amount of counterfeit fraud in excess of the amount of counterfeit fraud that normally would have been expected to have been reported on that group of accounts for the period in question. The Counterfeit Fraud Recovery Assessment thus violated the VIOR because the particular U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process did not incur, as a group, any amount of “incremental fraud” within the meaning of the VIOR.

57. In any event, the Counterfeit Fraud Recovery Assessment would be legally unenforceable even if it were valid under the VIOR, because the Counterfeit Fraud Recovery Assessment constitutes a penalty – rather than damages – for the Acquiring Banks allegedly having breached their contracts with Visa, and as such it is legally unenforceable under applicable law. Visa does not even pretend that the Counterfeit Fraud Recovery Assessment represents the actual damages of *Visa itself* by reason of the Acquiring Banks’ alleged breaches of their contractual obligation to cause Genesco to comply with the requirements of the PCI DSS. To the contrary, by the ADCR’s very terms, the Counterfeit Fraud Recovery Assessment purports to constitute losses that *Visa’s U.S. issuers* incurred by reason of the Acquiring Banks’ alleged violations of their contractual obligation to Visa. But Visa’s U.S. issuers are not parties to or third-party beneficiaries of the contracts between the Acquiring Banks and Visa, so the

Acquiring Banks can have no breach-of-contract liability under those agreements for damages suffered by those issuers. And even if they could have such liability, the ADCR's provisions for Counterfeit Fraud Recovery do not purport to calculate the counterfeit losses that Visa issuers *actually* incur by reason of an account compromise event that results from a merchant's failure to be PCI DSS compliant – meaning that any liability arising under those provisions could only be sustained if the provisions were valid liquidated damages provisions. The ADCR's provisions for Counterfeit Fraud Recovery are not valid liquidated damages provisions, however, because (1) Counterfeit Fraud Recovery is not intended to be compensatory damages for counterfeit fraud losses incurred by *Visa* by reason of a Visa acquirer's failure to ensure its merchants' PCI DSS compliance, but rather is intended to compensate such counterfeit fraud losses incurred by *Visa's U.S. issuers*, who are not parties to or third-party beneficiaries of a Visa acquirer's contract with Visa; (2) the VIOR purport to afford Visa unbounded discretion to determine the imposition and calculate the amount of Counterfeit Fraud Recovery; (3) the amount of any counterfeit fraud losses that Visa and/or its U.S. issuers may actually incur by reason of a Visa acquirer's failure to ensure its merchants' PCI DSS compliance is not only reasonably estimable, but calculable to the penny, to the extent they incur any such losses at all; and (4) Counterfeit Fraud Recovery is not Visa's exclusive damages remedy by reason of a Visa acquirer's failure to ensure its merchants' PCI DSS compliance. Because the Counterfeit Fraud Recovery Assessment cannot be sustained as a valid award of either actual or liquidated damages by reason of the Acquiring Banks' alleged breaches of their contractual obligation to Visa to cause Genesco to comply with the PCI DSS, that assessment necessarily constitutes a penalty by reason of such alleged breaches, and as such it is unenforceable under applicable law regardless of whether it comports with the VIOR (which it does not).

Visa's Invalid Imposition and Collection of the Operating Expense Reimbursement Assessment

58. The Operating Expense Recovery Assessment directly violated the VIOR because Visa did not show (and indeed could not even reasonably have concluded), and in any event it was not the case, that (1) Genesco suffered a theft of cardholder data with respect to all the U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process (or for that matter even with respect to any particular U.S.-issued Alerted-On Account that Visa found to be so eligible); (2) Genesco committed a PCI DSS violation that allowed the theft of cardholder data with respect to all the U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process (or for that matter even with respect to any particular U.S.-issued Alerted-On Account that Visa found to be so eligible); and/or (3) Visa's U.S. Issuers incurred operating expenses with respect to the U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process (or for that matter any particular portion of the U.S.-issued Alerted-On Accounts that Visa found to be so eligible) as a result of the theft in question.

59. In regard to Paragraph 58(1) above, under the VIOR an account can be made eligible for Operating Expense Recovery pursuant to the ADCR process only if it suffers an "account compromise event." The term "account compromise event", as used in the ADCR, means an actual theft of cardholder data relative to the account in question. Visa did not show (and indeed could not even reasonably have concluded), and in any event it was not the case, that Genesco suffered a theft of cardholder data with respect to all the particular U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process (or for that matter even with respect to any particular U.S.-issued Alerted-On Account that Visa found to be so eligible). Indeed, with respect to some of the U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process, Visa found the Alerted-On Account in question to be so eligible

even though the forensic evidence affirmatively showed that those accounts *had not* been compromised during the Intrusion. Moreover, with respect to all of the other U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process, Visa found the Alerted-On Account in question to be so eligible even though there was no forensic evidence showing that those accounts had been compromised during the Intrusion. Accordingly, with respect to all (or at a minimum some) of the U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process, Visa did not show (and indeed could not even reasonably have concluded), and in any event it was not the case, that Genesco suffered an account compromise event as to those accounts. The Operating Expense Recovery Assessment thus violated the VIOR because all (or at a minimum some) of the Visa accounts on which the assessment is based were ineligible for the ADCR process by reason of their not having suffered an account compromise event.

60. Moreover, in further regard to Paragraph 58(1) above, certain of the U.S.-issued Alerted-On Accounts on which the Operating Expense Recovery Assessment is based could not even *possibly* have suffered an account compromise event during the course of the Intrusion, because reboots of the intruded-upon servers in the Genesco cardholder data environment caused any log files that may have contained data relative to those accounts to be overwritten by the intruder(s)' malware prior to the intruder(s)' having an opportunity to exfiltrate the files from Genesco's network. Thus, even if the term "account compromise event" as used in the ADCR means merely a *possible* theft of cardholder data relative to the account in question, and not an *actual* theft of such data (which is not the case), as a result of such overwriting Genesco did not even suffer a *possible* theft of cardholder data with respect to many of the particular U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process. For this reason as

well, then, the Operating Expense Recovery Assessment violated the VIOR because even under a broad definition of the term “account compromise event” at least some of the Visa accounts on which the assessment is based were ineligible for the ADCR process by reason of their not having suffered such an event.

61. In regard to Paragraph 58(2) above, under the VIOR a Visa account can be made eligible for Operating Expense Recovery pursuant to the ADCR process only if the entity in question committed some violation of the PCI DSS that could have allowed the compromise (i.e., the theft) of the full contents of any track on the magnetic stripe of that particular account. Here, Visa did not show (and indeed could not even reasonably have concluded), and in any event it was not the case, that Genesco committed a PCI DSS violation that allowed the theft of cardholder data with respect to all the U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process (or for that matter even with respect to any particular U.S.-issued Alerted-On Account that Visa found to be so eligible). In particular, Visa did not show (and indeed could not even reasonably have concluded), and in any event it was not the case, that any PCI DSS violation on the part of Genesco is what enabled the intruder(s) to enter Genesco’s computer network or is what enabled them potentially to steal payment card account data from Genesco’s computer system. The Operating Expense Recovery Assessment thus violated the VIOR because all of the U.S.-issued Alerted-On Accounts on which the assessment is based were ineligible for the ADCR process by reason of their having been no PCI DSS violation by Genesco that could have allowed the compromise (i.e., the theft) of the full contents of any track on the magnetic stripe of that particular account.

62. In regard to Paragraph 58(3) above, under the VIOR a group of Visa accounts can form the basis for a Visa acquirer to be liable for Operating Expense Recovery pursuant to the

ADCR process only where, and only to the extent, Visa's U.S. issuers incurred operating expenses with respect to that particular group of accounts as a result of an account compromise event. There is no evidence, and Visa made no finding (and would have had no reasonable basis for making a finding), and in any event it was not the case, that Visa's U.S. issuers incurred any amount of operating expenses (much less operating expenses in an amount at least equal to the amount of the Operating Expense Recovery Assessment) by reason of the U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process (or for that matter any particular portion of the U.S.-issued Alerted-On Accounts that Visa found to be so eligible) having suffered an account compromise event. The Operating Expense Recovery Assessment thus violated the VIOR because Visa's U.S. issuers did not incur any amount of operating expenses (much less operating expenses in an amount at least equal to the amount of the Operating Expense Recovery Assessment) by reason of the U.S.-issued Alerted-On Accounts that Visa found to be eligible for the ADCR process having suffered an account compromise event.

63. In any event, the Operating Expense Recovery Assessment would be legally unenforceable even if they were valid under the VIOR, because the Operating Expense Recovery Assessment constitutes a penalty – rather than damages – for the Acquiring Banks' allegedly having breached their contracts with Visa, and as such it is legally unenforceable under applicable law. Visa does not even pretend that the Operating Expense Recovery Assessment represents the actual damages of *Visa itself* by reason of the Acquiring Banks' alleged breaches of their contractual obligation to cause Genesco to comply with the requirements of the PCI DSS. To the contrary, by the ADCR's very terms, the Operating Expense Recovery Assessment purports to constitute losses that *Visa's U.S. issuers* incurred by reason of the Acquiring Banks'

alleged violations of their contractual obligation to Visa. But Visa's U.S. issuers are not parties to or third-party beneficiaries of the contracts between the Acquiring Banks and Visa, so the Acquiring Banks can have no breach-of-contract liability under those agreements for damages suffered by those issuers. And even if they could have such liability, the ADCR's provisions for Operating Expense Recovery do not purport to calculate the counterfeit losses that Visa issuers *actually* incurred by reason of an account compromise event that results from a merchant's failure to be PCI DSS compliant – meaning that any liability arising under those provisions could only be sustained if the provisions were valid liquidated damages provisions. The ADCR's provisions for Operating Expense Recovery are not valid liquidated damages provisions, however, because (1) Operating Expense Recovery is not intended to be compensatory damages for operating expenses incurred by *Visa* by reason of a Visa acquirer's failure to ensure its merchants' PCI DSS compliance, but rather is intended to compensate such operating expenses incurred by *Visa's U.S. issuers*, who are not parties to or third-party beneficiaries of a Visa acquirer's contract with Visa; (2) the VIOR purport to afford Visa unbounded discretion to determine the imposition and calculate the amount of Operating Expense Recovery; (3) the amount of any operating expenses that Visa and/or its U.S. issuers may actually incur by reason of a Visa acquirer's failure to ensure its merchants' PCI DSS compliance is not only reasonably estimable, but calculable to the penny, to the extent they incurred any such losses at all; and (4) Operating Expense Recovery is not Visa's exclusive damages remedy by reason of a Visa acquirer's failure to ensure its merchants' PCI DSS compliance. Because the Operating Expense Recovery Assessment cannot be sustained as a valid award of either actual or liquidated damages by reason of the Acquiring Banks' alleged breaches of their contractual obligation to Visa to cause Genesco to comply with the PCI DSS, that assessment necessarily constitutes a penalty by

reason of such alleged breaches, and as such it is unenforceable under applicable law regardless of whether it comports with the VIOR (which it does not).

Visa's Invalid Imposition and Collection of the DCRS Assessment

64. The DCRS Assessment directly violates the VIOR because Visa did not show (and indeed could not even reasonably have concluded), and in any event it was not the case, that (1) Genesco suffered a theft of cardholder data with respect to all the non-U.S. issued Alerted-On Accounts that Visa found to be eligible for the DCRS process (or for that matter even with respect to any particular non-U.S. issued Alerted-On Account that Visa found to be so eligible); (2) Genesco committed a PCI DSS violation that allowed the theft of cardholder data with respect to all the non-U.S. issued Alerted-On Accounts that Visa found to be eligible for the DCRS process (or for that matter even with respect to any particular non-U.S. issued Alerted-On Account that Visa found to be so eligible); and/or (3) the non-U.S. issued Alerted-On Accounts that Visa found to be eligible for the DCRS process (or for that matter any particular portion of the non-U.S. issued Alerted-On Accounts that Visa found to be so eligible) thereafter incurred, as a group, an amount of counterfeit fraud in excess of the amount of counterfeit fraud that normally would have been expected to have been reported on that group of accounts for the period in question.

65. In regard to Paragraph 64(1) above, under the DCRS an account can be made eligible for the DCRS process only if it suffers a "data compromise event." The term "data compromise event", as used in the DCRS, means an actual theft of cardholder data relative to the account in question. Visa did not show (and indeed could not even reasonably have concluded), and in any event it was not the case, that Genesco suffered a theft of cardholder data with respect to all the particular non-U.S. issued Alerted-On Accounts that Visa found to be eligible for the

DCRS process (or for that matter even with respect to any particular non-U.S. issued Alerted-On Account that Visa found to be so eligible). Indeed, with respect to some of the non-U.S. issued Alerted-On Accounts that Visa found to be eligible for the DCRS process, Visa found the Alerted-On Account in question to be so eligible even though the forensic evidence affirmatively showed that those accounts *had not* been compromised during the Intrusion. Moreover, with respect to all of the other non-U.S. issued Alerted-On Accounts that Visa found to be eligible for the DCRS process, Visa found the Alerted-On Account in question to be so eligible even though there was no forensic evidence showing that those accounts had been compromised during the Intrusion. Accordingly, with respect to all (or at a minimum some) of the non-U.S. issued Alerted-On Accounts that Visa found to be eligible for the DCRS process, Visa did not show (and indeed could not even reasonably have concluded), and in any event it was not the case, that Genesco suffered a data compromise event as to those accounts. The DCRS Assessment thus violated the VIOR because all (or at a minimum some) of the Visa accounts on which the assessment is based were ineligible for the DCRS process by reason of their not having suffered a data compromise event.

66. Moreover, in further regard to Paragraph 64(1) above, certain of the non-U.S. issued Alerted-On Accounts on which the DCRS Assessment is based could not even *possibly* have suffered a data compromise event during the course of the Intrusion, because reboots of the intruded-upon servers in the Genesco cardholder data environment caused any log files that may have contained data relative to those accounts to be overwritten by the intruder(s)' malware prior to the intruder(s)' having an opportunity to exfiltrate the files from Genesco's network. Thus, even if the term "data compromise event" as used in the DCRS means merely a *possible* theft of cardholder data relative to the account in question, and not an *actual* theft of such data (which is

not the case), as a result of such overwriting Genesco did not even suffer a *possible* theft of cardholder data with respect to many of the particular non-U.S. issued Alerted-On Accounts that Visa found to be eligible for the DCRS process. For this reason as well, then, the DCRS Assessment violated the DCRS because even under a broad definition of the term “data compromise event” at least some of the non-U.S.-issued Alerted-On Accounts on which the assessment is based were ineligible for the DCRS process by reason of their not having suffered such an event.

67. In regard to Paragraph 64(2) above, under the VIOR a Visa account can be made eligible for the DCRS process only if the entity in question committed some violation of the PCI DSS that could have allowed the compromise (i.e., the theft) of the full contents of any track on the magnetic stripe of that particular account. Here, Visa did not show (and indeed could not even reasonably have concluded), and in any event it was not the case, that Genesco committed a PCI DSS violation that allowed the theft of cardholder data with respect to all the non-U.S. issued Alerted-On Accounts that Visa found to be eligible for the DCRS process (or for that matter even with respect to any particular non-U.S. issued Alerted-On Account that Visa found to be so eligible). In particular, Visa did not show (and indeed could not even reasonably have concluded), and in any event it was not the case, that any PCI DSS violation on the part of Genesco is what enabled the intruder(s) to enter Genesco’s computer network or is what enabled them potentially to steal payment card account data from Genesco’s computer system. The DCRS Assessment thus violated the DCRS because all of the non-U.S.-issued Alerted-On Accounts on which the assessment is based were ineligible for the DCRS process by reason of their having been no PCI DSS violation by Genesco that could have allowed the compromise (i.e., the theft) of the full contents of any track on the magnetic stripe of that particular account.

68. In regard to Paragraph 64(3) above, under the DCRS a group of Visa accounts can form the basis for a Visa acquirer to be liable for the DCRS process only where “incremental fraud” is attributable to that particular group of accounts. Moreover, under the DCRS “incremental fraud” can properly be attributed to a particular group of Visa accounts only where that group of accounts incurred an amount of counterfeit fraud in excess of the amount of counterfeit fraud that normally would have been expected to have been reported on the accounts in question for the period in question. Visa did not show (and indeed could not even reasonably have concluded), and in any event it was not the case, that the non-U.S. issued Alerted-On Accounts that Visa found to be eligible for the DCRS process (or for that matter any particular portion of the non-U.S. issued Alerted-On Accounts that Visa found to be so eligible) incurred, as a group, an amount of counterfeit fraud in excess of the amount of counterfeit fraud that normally would have been expected to have been reported on that group of accounts for the period in question. The DCRS Assessment thus violated the DCRS because the particular non-U.S. issued Alerted-On Accounts that Visa found to be eligible for the DCRS process did not incur, as a group, any amount of “incremental fraud” within the meaning of the VIOR.

69. Moreover, the DCRS Assessment is invalid to the extent it included Alerted-On Accounts issued by Visa Europe issuers. The VIOR are explicit in stating that members of Visa Europe are separate from Visa, Inc. and therefore separately governed by the Operating Regulations of Visa Europe. Thus, nothing in the DCRS process, or anywhere else in the VIOR, makes accounts issued by Visa Europe issuers eligible for the DCRS process

70. In any event, the DCRS Assessment would be legally unenforceable even if it were valid under the VIOR, because the DCRS Assessment constitutes a penalty – rather than damages – for the Acquiring Banks’ allegedly having breached their contracts with Visa, and as

such it is legally unenforceable under applicable law. Visa does not even pretend that the DCRS Assessment represents the actual damages of *Visa itself* by reason of the Acquiring Banks' alleged breaches of their contractual obligation to cause Genesco to comply with the requirements of the PCI DSS. To the contrary, by the DCRS's very terms, the DCRS Assessment purports to constitute losses that *Visa's non-U.S. issuers* incurred by reason of the Acquiring Banks' alleged violations of their contractual obligation to Visa. But Visa's non-U.S. issuers are not parties to or third-party beneficiaries of the contracts between the Acquiring Banks and Visa, so the Acquiring Banks can have no breach-of-contract liability under those agreements for damages suffered by those issuers. And even if they could have such liability, DCRS's provisions do not purport to calculate the counterfeit losses that Visa issuers *actually* incur by reason of a data compromise event that results from a merchant's failure to be PCI DSS compliant – meaning that any liability arising under these provisions could only be sustained if the provisions were valid liquidated damages provisions. The DCRS's provisions are not valid liquidated damages provisions, however, because (1) DCRS liability is not intended to be compensatory damages for counterfeit fraud losses incurred by *Visa* by reason of a Visa acquirer's failure to ensure its merchants' PCI DSS compliance, but rather is intended to compensate such counterfeit fraud losses incurred by *Visa's non-U.S. issuers*, who are not parties to or third-party beneficiaries of a Visa acquirer's contract with Visa; (2) the VIOR purport to afford Visa unbounded discretion to determine the imposition and calculate the amounts of liability pursuant to the DCRS process; (3) the amount of any counterfeit fraud losses that Visa and/or its non-U.S. issuers may actually incur by reason of a Visa acquirer's failure to ensure its merchants' PCI DSS compliance is not only reasonably estimable, but calculable to the penny, to the extent they incur any such losses at all; and (4) DCRS liability is not Visa's exclusive

damages remedy by reason of a Visa acquirer's failure to ensure its merchants' PCI DSS compliance. Because the DCRS Assessment cannot be sustained as a valid award of either actual or liquidated damages by reason of the Acquiring Banks' alleged breaches of their contractual obligation to Visa to cause Genesco to comply with the PCI DSS, that assessment necessarily constitutes a penalty by reason of such alleged breaches, and as such it is unenforceable under applicable law regardless of whether it comports with the VIOR (which it does not).

FIRST CAUSE OF ACTION

(Breach of Contract – Non-Compliance Fines)

71. Genesco repeats and incorporates herein the allegations set forth in paragraphs 1 through 70 above.

72. A valid contract exists between the Acquiring Banks and Visa under which Visa was and is bound to comply with the VIOR.

73. The Non-Compliance Fines are not authorized by the VIOR.

74. The Non-Compliance Fines, even were they authorized by the VIOR (they were not and are not), are unenforceable under applicable law because they constitute contractual penalties for the Acquiring Banks' alleged breaches of their contracts with Visa.

75. By imposing the Non-Compliance Fines on, and collecting the Non-Compliance Fines from, the Acquiring Banks, Visa breached its contractual obligation to comply with the VIOR.

76. Genesco was obligated to indemnify the Acquiring Banks, and pursuant to such indemnification obligation Genesco reimbursed the Acquiring Banks, for the Non-Compliance Fines, even though such collection was unlawful on Visa's part.

77. Wells Fargo assigned to Genesco any and all rights, claims, or causes of actions that Wells Fargo may have against Visa to obtain reimbursement of any portion of the Non-Compliance Fines.

78. Because Genesco paid the Acquiring Banks the amount of the Non-Compliance Fines pursuant to a legal indemnity obligation, it was not a volunteer.

79. As a result of its payment to the Acquiring Banks of an amount primarily owed to them by Visa, Genesco has also become equitably subrogated to the Acquiring Banks' right of recovery against Visa of the Non-Compliance Fines.

80. Accordingly, Genesco is entitled to damages in amounts to be determined at trial, but not less than the full amount of the Non-Compliance Fines (\$10,000) together with any amounts incidental to the Non-Compliance Fines that Visa has imposed on and collected from the Acquiring Banks and that Genesco has in turn paid pursuant to its indemnity obligation to the Acquiring Banks.

SECOND CAUSE OF ACTION

(Breach of Contract – Wells Fargo Assessments)

81. Genesco repeats and incorporates herein the allegations set forth in paragraphs 1 through 70 above.

82. A valid contract exists between Wells Fargo and Visa under which Visa was and is bound to comply with the VIOR.

83. Wells Fargo has fully performed its obligations under its contract with Visa.

84. Visa was contractually obligated under the VIOR to pay Wells Fargo, as part of the daily flow of funds from Visa to Wells Fargo, the amounts it withheld from Wells Fargo in satisfaction of the Wells Fargo Assessments.

85. Any and all conditions precedent to Visa's payment obligations were fulfilled.
86. Only if the Wells Fargo Assessments were both authorized by the VIOR and enforceable under applicable law would Visa have been authorized to collect the Wells Fargo Assessments by withholding the funds otherwise owed to Wells Fargo.
87. The Wells Fargo Assessments were not authorized by the VIOR.
88. The Wells Fargo Assessments, even were they authorized by the VIOR (they were not and are not), are unenforceable under applicable law because they constitute contractual penalties for Wells Fargo's alleged breach of its contract with Visa.
89. Accordingly, Visa was contractually obligated to Wells Fargo under the VIOR for the amounts it withheld from Wells Fargo in satisfaction of the Wells Fargo Assessments, and Visa breached its contract with Wells Fargo by failing to meet that contractual obligation.
90. Visa was (and is) therefore liable to Wells Fargo for the amount of the Wells Fargo Assessments.
91. Visa, in equity and good conscience, should discharge that liability. It is primarily answerable to Wells Fargo for the amounts of the Wells Fargo Assessments.
92. Wells Fargo responded to Visa's wrongful imposition and collection of the Wells Fargo Assessments by withholding the amount of the Wells Fargo Assessments from Genesco pursuant to a legal obligation of Genesco to indemnify Wells Fargo for any such wrongful takings by Visa.
93. Wells Fargo assigned to Genesco any and all rights, claims, or causes of actions that Wells Fargo may have against Visa to obtain reimbursement of any portion of the Wells Fargo Assessments.

94. Because Genesco paid Wells Fargo the amount of the Wells Fargo Assessments pursuant to a legal indemnity obligation, it was not a volunteer.

95. As a result of its payment to Wells Fargo of amounts primarily owed to Wells Fargo by Visa, Genesco has also become equitably subrogated to Wells Fargo's right of recovery against Visa of the damages Wells Fargo incurred by reason of Visa's breach of its contract with Wells Fargo in regard to the Wells Fargo Assessments.

96. Genesco is entitled to money damages for Visa's breach of its contract with Wells Fargo in regard to the Wells Fargo Assessments in an amount to be determined at trial, but not less than the full amount of the Wells Fargo Assessments against Wells Fargo (\$11,946,490.23) together with any amounts incidental to the Wells Fargo Assessments that Genesco has in turn paid pursuant to its indemnity obligation to Wells Fargo.

THIRD CAUSE OF ACTION

(Breach of the Implied Covenant of Good Faith and Fair Dealing – Wells Fargo Assessments)

97. Genesco repeats and incorporates herein the allegations set forth in paragraphs 1 through 70 above.

98. A valid contract exists between Wells Fargo and Visa under which Visa was and is bound to comply with the VIOR.

99. The VIOR purport to empower Visa with the right to unilaterally determine the rights of Visa and obligations of Visa Members under certain aspects of the VIOR including, without limitation, certain such aspects relating to the imposition and amount of CISP non-compliance fines, Counterfeit Fraud Recovery, Operating Expense Recovery, and DCRS Recovery. To the extent the VIOR purport to grant Visa the unilateral discretion to determine the rights and obligations of Visa and Wells Fargo respectively under the VIOR regarding any

aspect of Visa's imposition and/or collection of the Wells Fargo Assessments, those provisions are unenforceable as a matter of law. However, to the extent any of those provisions are found to be enforceable to any extent (which they are not), Visa acted unfairly without good faith by the manner in which it exercised such discretion in imposing the Wells Fargo Assessments against Wells Fargo, and collection of the Wells Fargo Assessments from Wells Fargo, and by doing so deprived Wells Fargo of the benefits of its contract with Visa. Thus Visa violated the implied covenant of good faith and fair dealing.

100. Wells Fargo has fully performed its obligations under its contract with Visa.

101. Visa was contractually obligated under the VIOR to pay Wells Fargo, as part of the daily flow of funds from Visa to Wells Fargo, the amounts it withheld from Wells Fargo in satisfaction of the Wells Fargo Assessments.

102. Any and all conditions precedent to Visa's payment obligations were fulfilled.

103. Only if the Wells Fargo Assessments were both authorized by the VIOR and enforceable under applicable law would Visa have been authorized to collect the Wells Fargo Assessments by withholding the funds otherwise owed to Wells Fargo.

104. The Wells Fargo Assessments were not authorized by the VIOR.

105. Accordingly, Visa was contractually obligated to Wells Fargo under the VIOR for the amounts it withheld from Wells Fargo in satisfaction of the Wells Fargo Assessments, and Visa violated the implied covenant of good faith and fair dealing by unfairly interfering with Wells Fargo's right to receive those amounts.

106. Visa was (and is) therefore liable to Wells Fargo for the amount of the Wells Fargo Assessments.

107. Visa, in equity and good conscience, should discharge that liability. It is primarily answerable to Wells Fargo for the amounts of the Wells Fargo Assessments.

108. Wells Fargo responded to Visa's wrongful imposition and collection of the Wells Fargo Assessments by withholding the amount of the Wells Fargo Assessments from Genesco pursuant to a legal obligation of Genesco to indemnify Wells Fargo for any such wrongful takings by Visa.

109. Wells Fargo assigned to Genesco any and all rights, claims, or causes of actions that Wells Fargo may have against Visa to obtain reimbursement of any portion of the Wells Fargo Assessments.

110. Because Genesco paid Wells Fargo the amount of the Wells Fargo Assessments pursuant to a legal indemnity obligation, it was not a volunteer.

111. As a result of its payment to Wells Fargo of amounts primarily owed to Wells Fargo by Visa in regard to the Wells Fargo Assessments, Genesco has also become equitably subrogated to Wells Fargo's right of recovery against Visa of the damages Wells Fargo incurred by reason of Visa's breach of the implied covenant of good faith and fair dealing.

112. Genesco is entitled to money damages for Visa's breach of the implied covenant of good faith and fair dealing in regard to the Wells Fargo Assessments in an amount to be determined at trial, but not less than the full amount of the Wells Fargo Assessments (\$11,946,490.23) together with any amounts incidental to the Wells Fargo Assessments that Visa has imposed on and collected from Wells Fargo and that Genesco has in turn paid pursuant to its indemnity obligation to Wells Fargo.

FOURTH CAUSE OF ACTION

(Breach of Contract – Fifth Third Assessments)

113. Genesco repeats and incorporates herein the allegations set forth in paragraphs 1 through 70 above.

114. A valid contract exists between Fifth Third and Visa under which Visa was and is bound to comply with the VIOR.

115. Fifth Third has fully performed its obligations under its contract with Visa.

116. Visa was contractually obligated under the VIOR to pay Fifth Third, as part of the daily flow of funds from Visa to Fifth Third, the amounts it withheld from Fifth Third in satisfaction of the Fifth Third Assessments.

117. Any and all conditions precedent to Visa's payment obligations were fulfilled.

118. Only if the Fifth Third Assessments were both authorized by the VIOR and enforceable under applicable law would Visa have been authorized to collect the Fifth Third Assessments by withholding the funds otherwise owed to Fifth Third.

119. The Fifth Third Assessments were not authorized by the VIOR.

120. The Fifth Third Assessments, even were they authorized by the VIOR (they were not and are not), are unenforceable under applicable law because they constitute contractual penalties for Fifth Third's alleged breach of its contract with Visa.

121. Accordingly, Visa was contractually obligated to Fifth Third under the VIOR for the amounts it withheld from Fifth Third in satisfaction of the Fifth Third Assessments, and Visa breached its contract with Fifth Third by failing to meet that contractual obligation.

122. Visa was (and is) therefore liable to Fifth Third for the amount of the Fifth Third Assessments.

123. Visa, in equity and good conscience, should discharge that liability. It is primarily answerable to Fifth Third for the amounts of the Fifth Third Assessments.

124. Fifth Third responded to Visa's wrongful imposition and collection of the Fifth Third Assessments by withholding the amount of the Fifth Third Assessments from Genesco pursuant to a legal obligation of Genesco to indemnify Fifth Third for any such wrongful takings by Visa.

125. Because Genesco paid Fifth Third the amount of the Assessments pursuant to a legal indemnity obligation, it was not a volunteer.

126. As a result of its payment to Fifth Third of amounts primarily owed to Fifth Third by Visa, Genesco has become equitably subrogated to Fifth Third's right of recovery against Visa of the damages Fifth Third incurred by reason of Visa's breach of its contract with Fifth Third in regard to the Fifth Third Assessments.

127. Genesco is entitled to money damages for Visa's breach of its contract with Fifth Third in regard to the Fifth Third Assessments in an amount to be determined at trial, but not less than the full amount of the Fifth Third Assessments against Fifth Third (\$1,342,409.93) together with any amounts incidental to the Fifth Third Assessments that Genesco has in turn paid pursuant to its indemnity obligation to Fifth Third.

FIFTH CAUSE OF ACTION

(Breach of the Implied Covenant of Good Faith and Fair Dealing – Fifth Third Assessments)

128. Genesco repeats and incorporates herein the allegations set forth in paragraphs 1 through 70 above.

129. A valid contract exists between Fifth Third and Visa under which Visa was and is bound to comply with the VIOR.

130. The VIOR purport to empower Visa with the right to unilaterally determine the rights of Visa and obligations of Visa Members under certain aspects of the VIOR, including,

without limitation, certain aspects relating to the imposition and amount of CISP non-compliance fines, Counterfeit Fraud Recovery, Operating Expense Recovery, and DCRS Recovery. To the extent the VIOR purport to grant Visa the unilateral discretion to determine the rights and obligations of Visa and Fifth Third respectively under the VIOR regarding any aspect of Visa's imposition and/or collection of the Fifth Third Assessments, those provisions are unenforceable as a matter of law. However, to the extent any of those provisions are found to be enforceable to any extent (which they are not), Visa acted unfairly without good faith by the manner in which it exercised such discretion in imposing the Fifth Third Assessments against Fifth Third, and collecting the Fifth Third Assessments from Fifth Third, and by doing so deprived Fifth Third of the benefits of its contract with Visa. Thus Visa breached the implied covenant of good faith and fair dealing.

131. Fifth Third has fully performed its obligations under its contract with Visa.

132. Visa was contractually obligated under the VIOR to pay Fifth Third, as part of the daily flow of funds from Visa to Fifth Third, the amounts it withheld from Fifth Third in satisfaction of the Fifth Third Assessments.

133. Any and all conditions precedent to Visa's payment obligations were fulfilled.

134. Only if the Fifth Third Assessments were both authorized by the VIOR and enforceable under applicable law would Visa have been authorized to collect the Fifth Third Assessments by withholding the funds otherwise owed to Fifth Third.

135. The Assessments were not authorized by the VIOR.

136. Accordingly, Visa was contractually obligated to Fifth Third under the VIOR for the amounts it withheld from Fifth Third in satisfaction of the Fifth Third Assessments, and Visa

violated the implied covenant of good faith and fair dealing by unfairly interfering with Fifth Third's right to receive those amounts.

137. Visa was (and is) therefore liable to Fifth Third for the amount of the Fifth Third Assessments wrongfully withheld from Fifth Third.

138. Visa, in equity and good conscience, should discharge that liability. It is primarily answerable to Fifth Third for the amounts of the Fifth Third Assessments.

139. Fifth Third responded to Visa's wrongful imposition and collection of the Fifth Third Assessments by withholding the amount of the Fifth Third Assessments from Genesco pursuant to a legal obligation of Genesco to indemnify Fifth Third for any such wrongful takings by Visa.

140. Because Genesco paid Fifth Third the amount of the Fifth Third Assessments pursuant to a legal indemnity obligation, it was not a volunteer.

141. As a result of its payment to Fifth Third of amounts primarily owed to Fifth Third by Visa in regard to the Fifth Third Assessments, Genesco has also become equitably subrogated to Fifth Third's right of recovery against Visa of the damages Fifth Third incurred by reason of Visa's breach of the implied covenant of good faith and fair dealing.

142. Genesco is entitled to money damages for Visa's breach of the implied covenant of good faith and fair dealing in regard to the Fifth Third Assessments in an amount to be determined at trial, but not less than the full amount of the Fifth Third Assessments against Fifth Third (\$1,342,409.93) together with any amounts incidental to the Fifth Third Assessments that Visa has imposed on and collected from Fifth Third and that Genesco has in turn paid pursuant to its indemnity obligation to Fifth Third.

SIXTH CAUSE OF ACTION

(Violation of California Unfair Business Practices Act, CAL. BPC. CODE § 17200 – Non-Compliance Fines and Assessments)

143. Genesco repeats and incorporates herein the allegations set forth in paragraphs 1 through 70 above.

144. Visa is prohibited from engaging in “unlawful, unfair or fraudulent business practices” by California Business & Professions Code §§17200, *et seq.*

145. Visa knew, or had reason to know, that by imposing the Non-Compliance Fines and the Assessments on, and by collecting the Non-Compliance Fines and the Assessments from, the Acquiring Banks, the amounts of the Assessments, would be passed through to Genesco by the Acquiring Banks.

146. By imposing the Non-Compliance Fines and the Assessments, and by collecting the Non-Compliance Fines and the Assessments, Visa deliberately harmed Genesco. Because the Non-Compliance Fines and the Assessments against the Acquiring Banks are invalid under the VIOR and applicable law, Visa lacks justification for having imposed such harm on Genesco and acted unfairly in doing so. Accordingly, Visa’s imposition and collection of the Non-Compliance Fines and the Assessments was an “unfair” business practice in violation of the California Business & Professions Code.

147. By imposing the Non-Compliance Fines and the Assessments, and by collecting the Non-Compliance Fines and the Assessments, Visa misrepresented to the Acquiring Banks that these amounts were due and owing to Visa under the VIOR and applicable law. In doing so, Visa knew or should have known that the Assessments and the Non-Compliance Fines would be

passed through to Genesco. Because the Non-Compliance Fines and the Assessments are invalid under the VIOR and applicable law, the Non-Compliance Fines and the Assessments was a “fraudulent” business practice in violation of the California Business & Professions Code.

148. Visa wrongfully obtained money from Genesco in the amount of \$13,298,900.16 by engaging in “unlawful, unfair or fraudulent business practices” as described above.

149. Genesco is entitled to the restoration of all money and property wrongfully collected by Visa from Genesco by means of Visa’s above-described unfair and/or fraudulent business practices, including money lost by Genesco as a result of Visa’s breach of its contracts with the Acquiring Banks in an amount to be determined at trial, but not less than the full amount of both the Assessments and the Non-Compliance Fines (\$13,298,900.16) together with any amounts incidental to Visa’s imposition of the Assessments and the Non-Compliance Fines that Visa has imposed on and collected from the Acquiring Banks and that Genesco has in turn paid pursuant to its indemnity obligation to the Acquiring Banks.

SEVENTH CAUSE OF ACTION

(Money Had and Received or Restitution/Unjust Enrichment – Non-Compliance Fines and Assessments)

150. Genesco repeats and incorporates herein the allegations set forth in paragraphs 1 through 70 above.

151. By imposing the Non-Compliance Fines and the Assessments on, and by collecting the Non-Compliance Fines and the Assessments from, the Acquiring Banks without any contractual or lawful basis for so doing, Visa was unjustly enriched and received money meant to be used for the benefit of Genesco.

152. This enrichment came at the expense of Genesco, who Visa knew would be left to pay the Assessments and the Non-Compliance Fines, once Visa wrongfully collected them,

because of Genesco's contractual obligation to indemnify Wells Fargo and Fifth Third against the Assessments and the Non-Compliance Fines notwithstanding their wrongful nature.

153. By reason of Visa's wrongful imposition and collection of the Assessments and the Non-Compliance Fines, and the Acquiring Banks' subsequent collection of the amount of the Assessments and the Non-Compliance Fines from Genesco, Visa now possesses funds that ultimately and rightfully belong to Genesco.

154. To allow Visa to retain such funds when Visa has no right to such funds would go against principles of right, justice, and morality.

155. Genesco is accordingly owed the amounts wrongfully imposed and collected by Visa and in turn indemnified by Genesco.

156. In the alternative, Visa was unjustly enriched by its actions in wrongfully imposing and collecting the Assessments and the Non-Compliance Fines, which violates basic principles of fairness, and equity and good conscience and requires that Visa make restitution to Genesco of the amounts by which Visa has been unjustly enriched at Genesco's expense.

157. Genesco is entitled to money damages and restitution by reason of Visa's improper collection and continued withholding of the Assessments and the Non-Compliance Fines—in the alternative, by reason of Visa's unjust enrichment—in an amount to be determined at trial, but not less than the full amount of the Assessments and the Non-Compliance Fines (\$13,298,900.16) together with any amounts incidental to the Assessments and the Non-Compliance Fines that Visa has imposed on and collected from the Acquiring Banks and that Genesco has in turn paid pursuant to its indemnity obligation to the Acquiring Banks.

WHEREFORE, Genesco demands judgment against Defendant Visa as follows:

A. On the First Cause of Action, damages in amounts to be determined at trial, but not less than the full amount of the Non-Compliance Fines (\$10,000) together with any amounts incidental to the Non-Compliance Fines that Visa has imposed on and collected from the Acquiring Banks and that Genesco has in turn paid pursuant to its indemnity obligation to the Acquiring Banks;

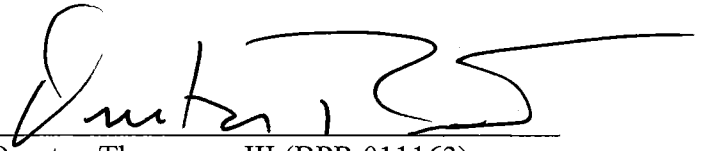
B. On the Second and Third Causes of Action, damages in amounts to be determined at trial, but not less than the full amount of the Wells Fargo Assessments (\$11,946,490.23) together with any amounts incidental to the Wells Fargo Assessments that Visa has imposed on and collected from Wells Fargo and that Genesco has in turn paid pursuant to its indemnity obligation to Wells Fargo;

C. On the Fourth and Fifth Causes of Action, damages in amounts to be determined at trial, but not less than the full amount of the Fifth Third Assessments (\$1,342,409.93) together with any amounts incidental to the Fifth Third Assessments that Visa has imposed on and collected from Fifth Third and that Genesco has in turn paid pursuant to its indemnity obligation to Fifth Third;

D. On the Sixth and Seventh Causes of Action, damages in amounts to be determined at trial, but not less than the full amount of the Assessments and the Non-Compliance Fines (\$13,298,900.16) together with any amounts incidental to the Assessments and/or to the Non-Compliance Fines that Visa has imposed on and collected from the Acquiring Banks and that Genesco has in turn paid pursuant to its indemnity obligation to the Acquiring Banks;

E. Such other and further relief the Court may deem appropriate.

Respectfully Submitted,



Overton Thompson III (BPR 011163)

(othompson@bassberry.com)

Wendee M. Hilderbrand (BPR 023688)

(whilderbrand@bassberry.com)

BASS, BERRY & SIMS PLC

150 Third Avenue South, Suite 2800

Nashville, TN 37201

(615) 742-7730 – Telephone

(615) 742-2804 – Facsimile

OF COUNSEL:

Douglas H. Meal

Seth C. Harrington

Matthew P. Thomas

ROPES & GRAY LLP

Prudential Tower

800 Boylston St.

Boston MA 02199-3600

(617) 951-7000

Attorneys for Plaintiff Genesco Inc.

11664234.1